Introduction

Cet ouvrage aborde en premier le sujet de la *Cyber Threat Intelligence* ou ce qu'on appelle le renseignement sur les cybermenaces. La Cyber Threat Intelligence est un moyen de défense et un savoir fondé sur des données probantes pour réduire l'écart entre les attaques avancées et les moyens de défense de l'organisation afin d'aider à la prise de décisions spécifiques ou d'éclairer l'ensemble des risques. Le chapitre 1 classe les types de Cyber Threat Intelligence existants et établit des distinctions entre eux, en mettant particulièrement l'accent sur les renseignements sur les menaces de nature technique ainsi que sur les dernières recherches, tendances et normes émergentes.

En cybersécurité, le partage d'informations est primordial pour une gestion efficace et collective des menaces et des vulnérabilités. Cependant, et compte tenu du caractère sensible de ces informations, les organisations sont souvent réticentes à les partager avec leurs pairs lorsqu'elles ne se trouvent pas dans un environnement fiable. Le recours à la confiance, combinée à de nouveaux services du *Cloud*, constitue actuellement une solution pour améliorer la réponse collective aux nouvelles menaces. Pour approfondir cette approche, le chapitre 2 traite de la confiance numérique et identifie les mécanismes qui sous-tendent les systèmes de gestion de la confiance. Il introduit les concepts de base de gestion de la confiance, classe et analyse plusieurs systèmes de gestion de la confiance. Ce chapitre montre comment les concepts de gestion de la confiance sont utilisés dans les systèmes récents pour relever les nouveaux défis posés par le *Cloud Computing.*

Lorsque les menaces ne sont pas bien traitées, toute vulnérabilité peut être exploitée et générer des coûts pour l'entreprise. Ces coûts peuvent être de nature humaine, technique et financière. Ainsi, pour faire face à ces menaces, une approche

---

Introduction rédigée par Wiem TOUNSI.

préventive visant à analyser les risques est primordiale. C'est l'objet du chapitre 3 qui présente une méthode complète d'analyse des risques des systèmes d'information déployée sur différents réseaux. Cette méthode est applicable aux extensions des normes et méthodes de gestion des risques existantes tout en se basant sur celles-ci.

Enfin, une approche de détection basée sur l'analyse dynamique et statique est définie dans le chapitre 4 pour défendre les données sensibles des utilisateurs mobiles, contre les attaques de flux d'informations lancées par des applications tierces. Une approche formelle et technique basée sur un mécanisme de marquage des données est proposée pour gérer les flux de contrôle dans le code Java et le code natif des applications et pour résoudre le problème d'*undertainting*, notamment dans les systèmes Android.